

Amendments to the Specification:

Please amend the specification as follows:

Please replace the first full paragraph on page 35, lines 8-22, with the following rewritten paragraph:

The random number dependence determining section 122 determines whether or not the intermediate data changing request should be outputted to the intermediate data control section 123, based on stage data at each processing stage of the encrypting operation from the encrypting operation section 121. The random number dependence determining section 122 outputs the intermediate data changing request to the intermediate data changing request section 123, when it is determined that intermediate data changing request should ~~is~~ be outputted, that is, when the current stage of the encrypting operation is determined to be the stage to which a random number dependent operation should be applied.

Please replace the first full paragraph on page 37, lines 5-9, with the following rewritten paragraph:

The random number generating unit 140 generates the random numbers in response to the random number generating request from the encryption processing unit 120 ~~to~~ and outputs them to the encryption processing unit 120.

Please replace the paragraph bridging pages 50 and 51 (page 50, line 21 to page 51, line 7), with the following rewritten paragraph:

The random number dependence determining section 522 determines whether or not the delay time ~~determinating~~ determining request should be outputted to the delay control section 523, based on the encrypting operation state data from the encrypting operating section 521. The random number

dependence determining section 522 outputs the delay time determining request to the delay control section 523, when it is determined that the delay time determining request should be outputted, that is, when the current processing stage of the encrypting operation is determined to be the stage to which a random number dependent operation should be applied.

Please replace the paragraph bridging pages 55 and 56 (page 55, line 22 to page 56, line 4), with the following rewritten paragraph:

In the third embodiment, the random number dependent delay time is ~~appropriately~~ appropriately inserted in the encrypting operation. Therefore, the process time effective for the cryptanalysis is continuously changed. Thus, it is difficult to determine which of the process times is effective for the cryptanalysis. Therefore, the encrypting apparatus has the endurance to the cryptanalysis such as the simple power analysis and the power differential analysis.